

I, Brett E. Banner, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed with the FBI since November 1999 and I am currently assigned to the Milwaukee Division Child Exploitation Task Force (CETF). I am charged with conducting investigations of violations of Federal Law including the receipt, possession, distribution and production of child pornography; coercion and enticement of a minor to engage in sexual contact; and, the sexual exploitation and sexual abuse of minors. I have gained experience in the conduct of such investigations through prior investigations, formal training and in consultation with law enforcement partners in local, state and federal law enforcement agencies. Prior to my assignment with Milwaukee I was assigned to the Detroit Division where I was the administrator for the Mid-Michigan Computer Crimes Task Force from June 2004 to September 2009. This task force primarily investigated crimes against children matters. I have also been employed in the State of Wisconsin as a certified law enforcement officer from 1993 to 1999.
2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. I am very familiar with the investigation of IP address 65.30.43.173, and Jeffrey Feldman. I am the case agent assigned by the FBI to this investigation.
4. I am submitting this affidavit for the limited purpose of explaining some of the aspects of this investigation relevant to the pretrial motions filed and I do not set forth every fact related to or otherwise the product of this investigation known to me.
5. As part of a pre-search warrant investigation an undercover FBI agent in Milwaukee used the *RoundUp eMule* tool to investigate IP addresses involved in providing child

exploitation files for sharing through the eDonkey2000 (eD2K) and Kademia (KAD) P2P networks (the eDonkey/KAD network herein).

6. The investigation involved files made available to the public through the use of the eMule program.
7. The undercover FBI agent focused his search on IP address 65.30.43.173 as it was identified as being located in the Eastern District of Wisconsin, one of the jurisdictions I am charged to investigate for violations of federal law.
8. During the course of this investigation, neither the undercover FBI agent nor I distributed sexual exploitation of children files. These files are considered contraband.
9. I know from my investigation that the undercover FBI agent did not enable fake file sharing and was unable to complete a single source download.
10. At no time did the undercover agent attempt to remotely access and/or gather information from the defendant's computer that was not otherwise made available to the public through the defendant's use of eMule's file-sharing function.
11. I also know that no screen shots were taken by the undercover FBI agent and that no searches based on search words were conducted.
12. After the IP address 65.30.43.173 was identified, I, along with other law enforcement continued our investigation which I summarized in the search warrant affidavit.
13. These additional investigative steps required significant resources and work to be done in order for the FBI to be able to seek a search warrant. I personally participated in the investigation along with several other law enforcement officers.

14. For example, as I stated in the affidavit, the undercover law enforcement agent used Maxmind.com to determine that the IP address was registered to Time Warner / Road Runner. Maxmind.com is publically available website.
15. An administrative subpoena was issued by the FBI to Time Warner / Road Runner for the location and subscriber of the IP address during the undercover investigation. Time Warner reported that the IP address was assigned to Jeffrey Feldman, located at 2051 S. 102nd Street, Apt. E., West Allis, Wisconsin, which was within the investigative jurisdiction of the undercover officer. I used this information to determine the location of IP address 65.30.43.173.
16. As part of our continued investigation law enforcement visited the location and checked for any unsecured wireless connections.
17. I also reviewed administrative subpoenas and public records to establish that IP address 65.30.43.173 resolved to the defendant, Jeffrey Feldman. (Ex. A ¶¶ 9, 13-16) and to verify the exact location in Milwaukee where IP address 65.30.43.173 was located.
18. I know that the hash values of the files identified in the search warrant were converted from the eD2k MD4 hash value to the SHA-1 format as that is a format requested for the submission of files to the National Center for Missing and Exploited Children.
19. On January 22, 2013 I appeared before Magistrate Callahan and signed the affidavit in his presence. Magistrate Callahan authorized the search warrant and I was present when it was executed on January 24, 2013.
20. I know that the undercover officer verified that files identified in the eDonkey/KAD network as files containing child exploitation by viewing files with the exact same hash values and confirming that they contained child pornography. I described two of those

files in the search warrant affidavit so that the reviewing magistrate would know what files the hash values referred to. When law enforcement executed the search warrant we seized a desktop computer and numerous encrypted hard drives and related contraband. I also conducted a short interview of Feldman while an on-scene forensic examiner conducted preliminary forensic analyses of the computers, which was in large part thwarted by the inability to access the encrypted electronic storage equipment.

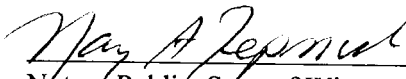
21. I am aware that the defendant and his expert were given access to the forensic evidence seized, were provided with electronic copies of files requested by the defense and given redacted copies of the 7 log files generated by *RoundUp eMule* investigation of this matter. In addition, the defense expert was provided with a hash conversion chart for all the files I noted in the search warrant affidavit.
22. The forensic examination of the desktop computer and numerous hard drives seized as part of the January 24, 2013 search warrant clearly shows that numerous files identified in the search warrant were downloaded onto the defendant's computer and/or hard drives prior to the dates of the undercover operation and that they were placed or used on the desktop computer and/or the hard drives long before the undercover investigation. Some files were found on the hard drives, others on the desktop computer while other files were found on both media. For example, the image associated with hash value 4A67D0742E2F7620E2B1F43B0A6F15E4FF97CCDE (one of the hash values I included in the search warrant affidavit) was found, pursuant to the forensic examination, in at least 9 different locations in the defendant's storage devices and were saved under different names.

23. Finally, the digital system located in Feldman's residence was approximately 19 terabytes in size. In comparison, the United States Library of Congress is 10 terabytes in size.



Brett Banner, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me this
24th day of March 2014.



Notary Public, State of Wisconsin

My commission is expires: 1/4/15.